Your response

About Barnardo's

Barnardo's is the UK's largest national children's charity. In 2022/23, we reached 373,200 children, young people, parents and carers through more than 800 services and partnerships across the UK. Our goal is to achieve better outcomes for more children. To achieve this, we work with partners to build stronger families, safer childhoods and positive futures.

Barnardo's has a long history of supporting all children through different forms of childhood harms, including child sexual abuse and exploitation. Barnardo's has supported children and young people affected by sexual abuse for over 25 years and now delivers specialist services in 45 locations across the UK. Our practitioners support children and young people's recovery by rebuilding their confidence and self-esteem, and by helping their families, schools and social networks make sense of what has happened. It is often long-term and complex work. We also work in partnership with other statutory and voluntary organisations to promote joined-up responses for children and their families, and strong support networks.

Barnardo's also hosts the Centre of expertise on child sexual abuse which seeks to reduce the impact of child sexual abuse through improved prevention and better response and provides support and guidance to thousands of professionals through its resources, training and research.

Overview of Barnardo's response

Barnardo's welcomes the opportunity to respond to the Illegal Harms Codes of Practice consultation, and recognises the scale and complexity of the task that Ofcom has in implementing and regulating the Online Safety Act. We have responded to the consultation questions below, but wanted to set out some fundamental concerns that we have with Ofcom's approach to the implementation of the Act, which we believe will undermine its intention, and ultimately will impact children's protection online.

Fundamentally, we feel that the measures set out in the proposed Codes of Practice are not ambitious enough, and do not achieve the Online Safety Act's overarching ambition to overhaul online platforms which at the moment are not working to protect children. Parliamentarians put a 'safety by design' approach at the heart of the Act, and included obligations for online platforms related to systems. This is not reflected in the Codes of Practice, which instead focus on individual items of content, and reflect back what many large platforms are already doing and do little to alter the status quo which the Online Safety Act was intended to improve.

One key barrier to this is Ofcom's seemingly very high evidential threshold, which is not defined in the Codes of Practice. As a result, the Codes of Practice only recommend measures that many platforms have already implemented, and that will not in themselves ensure safety by design. By giving preference to measures and tools that are already implemented by online platforms, Ofcom are failing to change the status quo, and to enable and encourage innovation in the child protection space.

This is also cemented by Ofcom's approach to proportionality. The approach taken is primarily a focus on economic costs, and to try to avoid imposing costs on companies. Whilst of course resource is an important proportionality consideration, it should not be the primary consideration. This is also not in line with the Act, which includes a focus on the levels of risk and the nature and severity of

harms caused by the platform. Ofcom's approach to proportionality takes into account the impacts on the online platform or service itself, but fails to consider what a proportionate response would be given the harm that these services are causing to children.

We feel that Ofcom are also placing too much trust in online platforms, and the Codes of Practice do not clearly set out how auditing or enforcement action would be taken. One of our key concerns is the 'self-assessment' that services are required to undertake to assess the level of risk they pose to children. For sites which are considered to be smaller, this assessment requires no external input. Many services which do pose a risk to children with regards to sexual abuse and exploitation would not be considered a large service, and the weak risk assessment obligations on such platforms potentially mean that they will not identify themselves as high- or multi-risk. As recent evidence from whistleblowers shows, many online platforms are aware of the risks that their platforms pose including regarding illegal content, yet choose not to take action.[1] To effectively enable child protection, it is key that Ofcom take a robust approach to the implementation of the Act, and ensure there are adequate checks and balances on self-assessment.

We are concerned about the lack of focus on child criminal exploitation in the Codes of Practice. Child criminal exploitation is a form of child abuse, and experiencing child criminal exploitation has a long-lasting impact on children, impacting both their mental health and physical health. Evidence shows that organised criminal gangs are increasingly using online platforms to target, groom and exploit children into criminal activity, which has particularly become prevalent since the COVID-19 pandemic and subsequent lockdowns.[2] This includes utilising tools and features on online platforms to criminally exploit children at all stages of child criminal exploitation. We would like to see child criminal exploitation identified in the Codes of Practice as an illegal harm that children can face online.

We are also concerned about the lack of engagement and consultation that Ofcom has conducted with children and young people in the development of the proposed Codes of Practice. Children and young people are the experts in their own experiences online and what can and should be done to protect them from harms. It is particularly important to consult with children and young people on the areas of the Codes of Practice which do directly impact them – including the measures designed to protect them from grooming and abuse and exploitation. Barnardo's would be happy to support with facilitating sessions for children and young people to meet with Ofcom to input into this and future Codes.

Finally, we are concerned that the measures suggested by Ofcom in the Codes of Practice do not include proactive technologies which online platforms should implement to detect, disrupt and remove 'new' and unknown child sexual abuse material, or the grooming of children online. We are supportive of measures that NSPCC have suggested in their consultation response regarding proactive technologies.

The Online Safety Act is a landmark piece of legislation which does offer a key step forward in ensuring that children are better protected online, including from illegal content. We do recognise that Ofcom has moved quickly in the development of this iteration of the first Codes, but we do urge Ofcom to ensure that speed of implementation does not hinder the quality and comprehensiveness of the measures.

---

[1] The Guardian, 2024. Meta has not done enough to safeguard children, whistleblower says

[2] Barnardo's, 2023. Invisible Children: Understanding the risk of the cost-of-living crisis and school holidays on child sexual and criminal exploitation.

Question (Volume 2)	Your response
Question 6.1: Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.	Overall, the evidence included in Volume 2 of the causes and impacts of online harm is robust, and accurately sets out the prevalence, causes and impact of child sexual abuse and exploitation online. We do however feel there are some gaps. <u>Child criminal exploitation</u> There is a lot of evidence on how exploiters use online platforms for child criminal exploitation, however this form of exploitation is not mentioned in Volume 2. We feel that this needs to be captured in the Codes of Practice as a way that children are groomed and abused online, particularly given the links between child criminal exploitation and child sexual abuse/ exploitation. Child Criminal Exploitation (CCE) is a form of child abuse. It is when a child under the age of 18 is encouraged, expected or required to take part in any activity that constitutes a criminal offence under British law.[3] CCE can take many forms, including 'county lines' (where children are coerced to carry drugs and weapons from one area to another to service complex drug supply chains), stealing or shoplifting to order, including perfumes, alcohol or cars, cannabis cultivation, and forced begging. CCE is intrinsically linked to child sexual abuse and exploitation. Many children experience both forms of exploitation. Online CCE has increased in recent years, with the COVID-19 pandemic and subsequent lockdowns increasing and exposing the scale of online CCE.[4] Exploiters can use online platforms at every stage of exploitation, including the initial contact with a child, grooming, exploitation, and to keep them trapped in cycles of exploitation. This includes exploiters advertising their associated lifestyles to their social media networks, for example posting pictures of luxury items and cash, a technique used to recruit and control victims. Barnardo's services support children whose exploitation started with initial contact via online platforms such as sharing posts aimed

[3] Barnardo's, 2023. Invisible Children: Understanding the risk of the cost-of-living crisis and school holidays on child sexual and criminal exploitation.
[4] Ibid.

Question (Volume 2)	Your response
	to lure children into trap-houses with money, trainers and weapons.[5] Research in 2019 showed that one in four (24%) of young people reported that they see illicit drugs advertised for sale on social media.[6] Further, in 2020, research by the Youth Endowment Fund found that 20% of young people had seen online content promoting gang membership in the previous 12 months, and 24% reported seeing content featuring carrying, using or promoting weapons.[7] Exploiters also use social media sites for 'remote mothering' – the ability to monitor where someone is, what they are doing, and who they are with at all times, via location tags, GPS tracking, pictures and video calling. The APPG for CCE and Knife Crime heard that perpetrators use features such as SnapMaps on Snapchat to track children.[8] Exploiters also use technology for online collateral. This, in particular, overlaps with child sexual abuse/ exploitation, with exploiters using indecent images of children, in addition to other incriminating images, videos, screenshots and voice notes, to ensure compliance, with the threat of sharing this material more widely. This is especially used to control girls, and 'subordinates' – often younger children. <u>Perpetrators of offences</u> In section 6C.31 of Volume 2, it sets out the backgrounds of perpetrators of child sexual abuse and exploitation. No reference is made to the growing evidence base which shows an association between the frequent viewing of legal pornographic content, including abusive and harmful content, and the progression to viewing child sexual abuse material and going on to groom and offend against children both online and offline. Evidence shows that the habitual viewing of this abusive and harmful pornographic content, including pornographic content which suggests or promotes child sexual abuse (i.e. 'barely legal' pornography and 'incest' pornography), can act as a gateway for users to offending, including for

[5] APPG on Child Criminal Exploitation and Knife Crime, 2022. Online Safety Bill and Child Criminal Exploitation
[6] Volteface, 2019. DM for details: selling drugs in the age of social media
[7] Youth Endowment Fund, 2022. Children, violence and vulnerability 2022: A Youth Endowment Fund report into young people's experiences of violence
[8] APPG on Child Criminal Exploitation and Knife Crime, 2022. Online Safety Bill and Child Criminal Exploitation

Question (Volume 2)	Your response
	offenders without a specific interest in children.[9] This was also supported by a study of 4,924 men from the UK, US and Australia, which found that those who reported sexual feelings towards or a history of offending against children were 11 times more likely to have watched violent pornography than men with no sexual feelings towards or history of offending against children.[10] Further, interviews with offenders who viewed child sexual abuse material in the UK indicate that most had not intentionally sought out child sexual abuse, but that it was a result of 'entrenched pornography use' and spiralling online behaviour.[11] Viewing legal pornographic content was also cited by the Centre of expertise on child sexual abuse as a common pathway to viewing child sexual abuse material online.[12] It is therefore important that the escalation pathways between viewing legal but violent and abusive pornographic content and then going on to view child sexual abuse material and/ or going on to groom children is made clear in Ofcom's evidence about these illegal harms.
Question 6.2: Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.	

[9] We Protect Global Alliance, 2023. Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response

[10] UNSW Australian Human Rights Institute, 2023. Identifying and understanding child sexual offending behaviours and attitudes among Australian men

[11] The Police Foundation, 2022. Turning the tide against online child sexual abuse

[12] Centre of expertise on child sexual abuse, 2023. Key messages from research on child sexual abuse by adults in online contexts

Question (Volume 3)	Your response
Question 8.1: Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice? Please provide underlying arguments and evidence of efficacy or risks to support your view.	
Question 8.2: Do you agree with the types of services that we propose the governance and accountability measures should apply to?	
Question 8.3: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?	
Question: 8.4: Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?	

Question (Volume 3)	Your response
Question 9.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	We are concerned that the risk assessment process that is proposed in the guidance is not robust enough to ensure that action will be taken to combat illegal content online, including child sexual abuse and exploitation. Firstly, we are concerned about the lack of external input and the auditing of risk assessments developed by online platforms. Under the 'core' inputs expected of online platforms, services are not required to consult external evidence and views about the risks that their platform poses. Whilst this is included as an 'enhanced' input, it is not expected of all services to complete this level of input for their risk assessment. In addition, the guidance does not set out how the risk assessments a platform completes will be audited, or checked by Ofcom to ensure they are accurate. Without mechanisms for this in place, it does appear that online platforms will be expected to 'mark their own homework', without oversight. As the implementation of other aspects of the Illegal Harms guidance rely on an online platform's risk level, this lack of oversight is concerning. Recent evidence provided by whistleblowers shows that online platforms can be aware of the risks of their services, but are not taking action. For example, Arturo Béjar, a former senior engineer and consultant at Meta, said that the platform has the tools at their proposal to make platforms safer for children, but have not implemented these changes.[13] Without input from external stakeholders and oversight from Ofcom, we are concerned that online platforms will be able to mark themselves as lower risk for illegal harms, even if evidence suggests otherwise. The guidance should be strengthened to ensure that it is a core input for external stakeholders to be consulted and external evidence to be reviewed. Ofcom's role in overseeing the risk assessments, and enforcement measures for ensuring risk assessments are appropriate, should be set out in the guidance. Further, we are concerned that the recommendation of updating a risk assessment every 12 months is not often enough. Technological developments, including those

[13] The Guardian, 2024. Meta has not done enough to safeguard children, whistleblower says

Question (Volume 3)	Your response
	which enable the sharing of child sexual abuse and exploitation content, can move very swiftly, and it's important that risk assessments are carried out often enough to capture new and emerging risks. For example, after first reporting that they were seeing AI-generated CSAM in June 2023, by September IWF reported that they had investigated 11,108 AI-generated images.[14] Currently, the guidance does suggest that reviews should be done more regularly than once a year if there is a change to the design of the service, but it does not include the same recommendation in relation to changes in content shared on the service– which is the case with the increase in AI-generated CSAM content. The guidance should therefore be updated so that risk assessments are updated more often, and to make it clear that risk assessments should be conducted more regularly if the type of content on a service change.
Question 9.2: Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?	
Question 9.3: Are the Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service?[15]	

[14] IWF, 2023. 'Worst nightmares' come true as predators are able to make thousands of new AI images of real child victims

[15] If you have comments or input related the links between different kinds of illegal harm and risk factors, please refer to Volume 2: Chapter 5 Summary of the causes and impacts of online harm).

Question (Volume 3)	Your response
Question 10.1: Do you have any comments on our draft record keeping and review guidance?	
Question 10.2: Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?	

Question (Volume 4)	Your response
Question 11.1: Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?	We are concerned that the proposed Codes of Practice will not go far enough to generate the real change that is needed to ensure protection from illegal harms, including CSA/E content, on online platforms. The proposed Codes of Practice lack ambition, and do not suggest anything inherently different from what many online platforms already implement to remove illegal content from their platforms. Coupled with the high weighting given to proportionality in the Codes of Practice, only large or high-risk services will be mandated to implement the proposed measures – many of which already do. For example, hash matching has been developed and used by platforms since 2003,[16] and is already used on large platforms such as Facebook and Instagram, with Meta developing their own hashing technology, PDQ hash function.[17] We are concerned that Ofcom's high bar for evidence before suggesting a measure hinders these proposed codes of practice, and future codes, to only suggest measures

[16] Ofcom, 2022. Overview of Perceptual Hashing Technology
[17] Ibid.

Question (Volume 4)	Your response
	that are already widely used and implemented – and therefore will only recommend what is already the status quo. The undue focus on proportionality also means that many small companies will be exempt from following many of the proposed measures. There is potential to let harmful and/ or risky small companies off the hook – such as collector sites for CSAM, where the risk is high and harmful. This is a particular concern when coupled with the 'safe harbour' clause in the Online Safety Act, which means that so long as services comply with what Ofcom propose, they would be deemed as compliant with the Act.[18] We are concerned that, if the Codes of Practice are not ambitious in the proposals they suggest and online platforms are not incentivised to further innovate, child protection will not improve. This will particularly be an issue regarding future emerging harms, such as those posed by the development of generative AI technologies and VR technologies. Further, it is concerning that none of the proposed measures for child sexual abuse/ exploitation apply to private messaging services. In Volume 2 of the guidance, Ofcom rightly sets out the risks that private messaging services can have regarding CSA/E, including the sharing of child sexual abuse material and the grooming of children. We know that, very often, when a child is groomed online, the offender can quickly move the conversation to private messaging services – including services with end-to-end encryption – to evade detection, known as off-platforming. Recent research found that, compared to men who had no sexual feelings or offending with children, those who had sexual feelings and offending with children were significantly more likely to use any of the eight privacy services included in the survey – including messaging services such as Telegram and Signal.[19] As well as grooming and sharing CSAM content on private messaging services, they can also be a forum for offenders to connect and share content or tips on offending, including 'paedophile manuals'. In 2022, the Child Rescue Coalition were able to collect over two million chat records, over 50,000 videos, over 2,000 images and over 250,00 individual accounts

[18] Society for Computers & Law, 2023. Ofcom issues first consultation under Online Safety Act 2023

[19] UNSW Australian Human Rights Institute, 2023. Identifying and understanding child sexual offending behaviours and attitudes among Australian men

Question (Volume 4)	Your response
	from criminal groups interested in child sexual exploitation from just one app-based end-to-end encrypted network.[20] Without illegal harms measures applying to private messaging services, one of the most risky elements of online platforms will remain unregulated. The Codes of Practice for CSA/E do not recommend any proactive measures that online platforms should implement to detect child sexual abuse material, or to detect bad actors on services, including those looking to groom and harm children. There is a major gap in the Codes of Practice which do not contain any measures to support the proactive detection of unknown or 'new' CSAM, or to detect and disrupt grooming. We are supportive of measures that NSPCC have suggested in their consultation response regarding proactive technologies, and would urge Ofcom to include these in future iterations of the Codes of Practice. Further, whilst identifying live streaming as a functionality which can particularly pose risks for the illegal harm of child sexual abuse/exploitation in volume 2, there are no measures required that relate to live streaming in the Codes of Practice. Livestreaming platforms enable abusers to control and coerce children into abuse, which can last for a long period of time and have a devastating impact on children. Such sites often have few or no measures in place to detect livestreamed child sexual abuse or exploitation – in August 2022, a transparency notice issued by the Australian e-Safety Commissioner found that three of four livestreaming or video call/ conferencing services they approached did not currently have the tools to detect livestreamed child sexual abuse or exploitation in place.[21] This gap is concerning, and must be addressed in future codes, including suggesting technologies which identify nudity in livestreams.

[20] We Protect Global Alliance, 2023. Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response

[21] Australian eSafety Commissioner, 2022. Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notices

Question (Volume 4)	Your response
Question 11.2: Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?	Barnardo's does not agree with the proportionality measures that have been set out in the proposed costs of practice. One of the key objectives of the Online Safety Act is to make the UK one of the safest places in the world to be online.[22] By only applying the most onerous measures to a small set of larger and riskier online platforms, including the measures designed to protect against CSA/E, the Codes of Practice will limit the Online Safety Act's ambition to better protect children. The approach that Ofcom has taken to proportionality is primarily economic, rather than considering the severity of harm a platform can have. This is not in line with the Online Safety Act, which requires Ofcom to, among other issues, consider the severity of harm posed by an online platform when considering proportionality. Many online platforms do have extremely high revenues, and economic costs on such platforms should not outweigh protection from illegal harms. The European Commission found that, in 2020, the total value of the world's top 100 online platforms was €10.5 trillion.[23] The abuse and grooming of children and the sharing of CSAM can take place anywhere online, no matter the size of the platform, and is prevalent. Research by the NSPCC found that, from 2018 – 2023, 150 different apps, games and websites were used to groom children online.[24] Further, information from Barnardo's child sexual abuse services found that two in three children and young people supported by the services were groomed online before they were sexually abused and/ or exploited.[25] The We Protect Global Alliance found that most detected child sexual abuse material on the surface web is found on image-hosting sites which often involve companies not widely used by mainstream consumers.[26] In 2022, 90% (228,927) of URLs identified by the IWF as displaying child

[22] Department for Science, Innovation and Technology, 2023. UK children and adults to be safer online as world-leading bill becomes law
[23] European Commission, 2019. How do online platforms shape our lives and businesses?
[24] NSPCC, 2023. 82% rise in online grooming crimes against children in the last 5 years.
[25] Barnardo's, 2019. Left to their own devices: young people, social media and mental health
[26] We Protect Global Alliance, 2023. Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response

Question (Volume 4)	Your response
	sexual abuse material were on openly accessible, free-to-use image hosting services.[27] Further, children can be groomed, abused and exploited on smaller platforms, and platforms that might not be considered 'high-risk'. There is an assumption in the Codes of Practice that small platforms mean less harm because of more limited reach, which we disagree with. This also downplays the severe harm that can occur on targeted, small sites – including grooming and the sharing of child sexual abuse material. We are concerned that, as smaller platforms are not required to implement many of the measures, they may be let 'off the hook' in terms of the measures, and when assessing risk. This could include gaming platforms which do not reach the high threshold of a 'large' service. Gaming platforms can be particularly high-risk due to perpetrators using them to groom children. The risk intelligence organisation, Crisp, found that offenders abusing children in these spaces are able to lock them into high-risk grooming conversations in as little as 19 seconds after the first message, with an average time of just 45 minutes.[28] Smaller services and online platforms which may not be considered as high-risk for CSA/E can also be used to groom and abuse/exploit children and to facilitate the sharing of CSAM. For example, a child was groomed on Spotify, despite the lack of direct messaging on the service.[29] This was done through the use of playlists to communicate, and playlist cover photos including CSAM. Barnardo's services have also supported a child who was abused and groomed through Lonely Planet. CSA/E offences take place across a range of platforms, not just sites that are large and may be considered 'high-risk'. It is crucial that economic-based proportionality measures do not prevent the Act from effectively being implemented across all services, resulting in children being harmed.

[27] IWF, 2023. IWF Annual Report 2022 #BehindTheScreens
[28] We Protect Global Alliance, 2023. Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response
[29] BBC News, 2023. Claims schoolgirl, 11, was groomed on Spotify

Question (Volume 4)	Your response
	Ultimately, weighing public safety from illegal harms against the costs to private companies do not align with Parliamentary expectations on what the regulatory framework should achieve. Speaking at the House of Lords Committee Stage debate on 2 May, Lord Parkinson, the Government Minister responsible for the Bill in the Lords said that all companies will have a responsibility to meet child safety duties where their services pose a risk to children: *"the provisions in the Bill on proportionality are important to ensure that the requirements in the child-safety duties are tailored to the size and capacity of providers. It is also essential that measures in codes of practice are technically feasible. This will ensure that the regulatory framework as a whole is workable for service providers and enforceable by Ofcom.* ***I reassure your Lordships that the smaller providers or providers with less capacity are still required to meet the child safety duties where their services pose a risk to children. They will need to put in place sufficiently stringent systems and processes that reflect the level of risk on their services, and will need to make sure that these systems and processes achieve the required outcomes of the child safety duty****. …* *The passage of the Bill should be taken as a clear message to providers that they need to begin preparing for regulation now—indeed, many are.* ***Responsible providers should already be factoring in regulatory compliance as part of their business costs.*** *Ofcom will continue to work with providers to ensure that the transition to the new regulatory framework will be as smooth as possible."*[30] Ofcom's approach suggests that implementing safety measures to tackle illegal harms could hinder a services' ability to compete, and that it could stifle innovation and competition. We disagree, and believe that safety from illegal harms online, including child sexual abuse and exploitation, should take precedent over economic considerations, especially considering the value of most of these platforms.

[30] Hansard, 2 May 2023. Online Safety Bill Lords Committee (4th Day) (Continued), Column 1485.

Question (Volume 4)	Your response
Question 11.3: Do you agree with our definition of large services?	
Question 11.4: Do you agree with our definition of multi-risk services?	
Question 11.6: Do you have any comments on the draft Codes of Practice themselves?[31]	
Question 11.7: Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?	
Question 12.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	Whilst we are supportive of the proposal to take down illegal content a site is aware of swiftly, we do not think that this goes far enough. We disagree with the high weighting given to economic proportionality, with just some services needing to set internal policies, resource its content moderation function, and ensure that the staff working on content moderation are adequately trained. As set out, illegal content, including CSA/E, can be present on any service, no matter the size or perceived risk to the content. It is important that all platforms are equipped to respond to such illegal content appropriately, not just a small fraction of online platforms.

[31] See Annexes 7 and 8.

Question (Volume 4)	Your response
	Further, we are concerned that the proposals do not include any measures related to actively detecting illegal content on a platform. Measures which allow a service to detect and tackle unknown illegal content should be included in the Codes of Practice.
Question 13.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	Whilst we are supportive of the proposal for search engines to deindex or downrank illegal content of which it is aware, again this does not go far enough. We are concerned that the proposals do not include any measures related to actively detecting illegal content on their search service. Measures which allow a search service to detect and tackle unknown illegal content should be included in the Codes of Practice.
Question 14.1: Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud keyword detection? Please provide the underlying arguments and evidence that support your views.	For the illegal harm of child sexual abuse/exploitation, we agree with Ofcom's proposals for the implementation of CSAM hash matching and CSAM URL detection. However, we do think that the proposals do not go far enough, and will not alter the status quo, with many large services already implementing these measures. As previously highlighted, we are concerned that the proportionality measures mean that the proposals will only apply to a small number of services. Many large services that will have to apply these services – such as Meta – already apply CSAM hash matching and CSAM URL detection,[32] and so it is unclear how the proposals will change the practice of online platforms, other than reinforcing the status quo. This is not in line with the overarching aims of the Online Safety Act, which was intended to improve child protection from the current norm. Once again we are also concerned about the high threshold for evidence which Ofcom has set before it suggests measures. The high threshold means that Ofcom are only recommending measures which the industry is already implementing, and discarding other measures. Further, it is concerning that these measures will not apply to private messaging services. As set out previously, CSAM and URL links that contain CSAM are often shared on private messaging forums – both when children are sexually

[32] Ofcom, 2022. Overview of Perceptual Hashing Technology

Question (Volume 4)	Your response
	exploited into sharing indecent imagery, and between offenders. By not applying these measures to private messaging services, a high proportion of the illegal harm will not be covered, detected or regulated – putting millions of children at risk. We are also concerned that the measures suggested to remove CSAM only focus on known images, and the technology will not detect unknown or 'new' CSAM. This technology does exist and is effective. For example, within just six months in 2021, services using Google's machine-learning tool to proactively identify 'new' CSAM classified over six billion images.[33] This technology would help millions of children who are victims of child sexual abuse, but is overlooked in the current measures. For CSAM URL detection, we are also concerned that the Codes of Practice do not reflect good practice. Whilst detecting and blocking URLs is important to prevent the spread of CSAM content, organisations including the IWF recommend that a splash page is served,[34] which: • Sets out the reason for the URL being blocked; • Highlights that viewing CSAM is a criminal offence; • Shares details of support organisations an individual could access to get help with their online behaviour (such as the Stop It Now! helpline); • Give an option to report any potential CSAM to the IWF. The Codes of Practice should reflect this good practice, and should be updated to set out that online platforms are expected to add a splash page.
Question 14.2: Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?	

[33] Google. Fighting child sexual abuse online
[34] IWF. URL Blocking: Good Practice

Question (Volume 4)	Your response
Question 14.3: Do you have any relevant evidence on: • The accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services; • The ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers; • The costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching[35] for CSAM URL detection; • The costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services; and • An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.	

[35] Fuzzy matching can allow a match between U2U content and a URL list, despite the text not being exactly the same.

Question (Volume 4)	Your response
Question 15.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 16.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 17.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 17.2: Do you have any evidence, in particular on the use of prompts, to guide further work in this area?	
Question 18.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	We welcome action to make it more difficult for adults to groom and abuse/exploit children on online platforms, however we do have concerns with the approach suggested in the proposed Codes of Practice. It is difficult to understand how the proposed measures would be implemented by online platforms without knowing how Ofcom will propose that online platforms should implement age assurance measures, as the proposed grooming measures are dependent on knowing whether a user is an adult or a child. We do agree with Ofcom that the self-declaration of a users' age is not an adequate method of assurance, but the age assurance measures Ofcom will be proposing should have been included in this

Question (Volume 4)	Your response
	version of the draft Codes of Practice, and we would recommend that they should be added to the next iteration of the Codes. We are also concerned again about the high weighting given to economic proportionality for these proposals. As set out in Ofcom's own evidence, children can be groomed and abused and exploited on a wide range of platforms. We are concerned that by only mandating that some platforms have to implement these measures, it will result in offenders moving to other, smaller and potentially less 'risky' services to groom children. Essentially this will just move the problem to sites which have fewer protections for children built into them. We are concerned that the proposed measures put the onus on child users to protect themselves from grooming, abuse and exploitation. It is important that children are given extra protections to prevent adult users that they do not know connecting and interacting with them, however by placing control with the child user to deactivate the default settings, it does still leave children at risk of abuse and exploitation particularly if they face offline pressures to do so. For example, this could include pressures faced from peers at school to conform with others and deactivate the settings. Research by Barnardo's found that children can feel pressured to be 'socially perfect' – to have many connections, and to keep up to date with the latest developments in technology.[36] Peer pressure could mean that children are influenced to 'follow trends' and deactivate these safety measures. Further, child abuse and exploitation often takes place both online and offline simultaneously, and features of online platforms can be used to track and control children who are being exploited.[37] We are concerned that a child could be coerced to deactivate the default settings by their exploiter – for example to reenable location sharing information – which can then be used to keep them trapped in a cycle of exploitation.

[36] Barnardo's, 2019. Left to their own devices: young people, social media and mental health

[37] Barnardo's, 2023. Invisible Children: Understanding the risk of the cost-of-living crisis and school holidays on child sexual and criminal exploitation.

Question (Volume 4)	Your response
	It is important that the information that services provide for children if they do look to deactivate the default settings are shared in an easily accessible, child-friendly way. The messaging should be inclusive, including of children with special educational needs and disabilities (SEND). Messaging should also provide information for children on how to seek help if they are being harmed or coerced to deactivate the default settings, including signposting to relevant support organisations. Further, proactive measures should be introduced by Ofcom which detect and disrupt grooming, and which are targeted at offenders rather than children. Automated content moderation technologies should be implemented to detect and disrupt grooming. Whilst alone machine learning is not enough to detect grooming, the use of this technology can significantly speed up how online grooming is spotted and moderated by flagging to human moderators. Further, keyword detection and machine learning offer technological solutions to improve grooming moderation. One example of this is Swansea University's Project DRAGON-S which they are working on with law enforcement to trial a new machine learning tool that will help them to quickly analyse chat logs to detect high-risk interactions between users.[38] Further, measures should be introduced which are targeted at identifying offenders and bad actors, rather than solely putting the onus on children's accounts. This should include tools to address the content that is shared by offenders, and also the way that they organise on and use online platforms. This could include recommending tools to identify offenders by detecting suspicious patterns of activity – such as adding accounts with content that sexualises children, or searching for egregious and coded terms on the platform. It should also include measures aimed to tackle the creation of fake profiles on online platforms, which are often used by offenders to connect with children. Accounts that are identified as offenders or bad actors should also be signposted to support organisations which provide help for those who are worried about their behaviour, including the Stop It Now! helpline.

[38] Swansea University. Project Dragon-S - Developing Resistance Against Grooming Online

Question (Volume 4)	Your response
Question 18.2: Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?	
Question 18.3: Are there other points within the user journey where under 18s should be informed of the risk of illegal content?	
Question 19.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 19.2: What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?	
Question 19.3: We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive. Are you aware of any other design parameters and choices that are proven to improve user safety?	

Question (Volume 4)	Your response
Question 20.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 20.2: Do you think the first two proposed measures should include requirements for how these controls are made known to users?	
Question 20.3: Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?	
Question 21.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	

Question (Volume 4)	Your response
Question 21.2: Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically: • What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)? What are the advantages and disadvantages of the different options, including any potential impact on other users? • How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed? • There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users. What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?	

Question (Volume 4)	Your response
Question 22.1: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.	
Question 23.1: Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?	
Question 23.2: Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?	
Question 23.3: We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?	
Question 24.1: Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard? If not, why not?	

Question (Volume 5)	Your response
Question 26.1: Do you agree with our proposals, including the detail of the drafting? What are the underlying arguments and evidence that inform your view.	
Question 26.2: Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?	
Question 26.3: What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?	

Question (Volume 6)	Your response
Question 28.1: Do you have any comments on our proposed approach to information gathering powers under the Act?	
Question 29.1: Do you have any comments on our draft Online Safety Enforcement Guidance?	

Question (Volume 6)	Your response

Question (Annex 13)	Your response
Question A13.1: Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?	
Question A13.2: If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	

Please complete this form in full and return to IHconsultation@ofcom.org.uk.